AUTHORITY AND INTEGRITY CHECK IN SYSTEMS LACKING A PUBLIC KEY

FIELD OF THE INVENTION

This invention relates to a system and method for verifying the authority and integrity of information, and more particularly to a system and method for verifying the authority and integrity of information when a public key is unavailable.

BACKGROUND OF THE INVENTION

In the field of information technology (IT) management, a large number of computing platforms, such as personal computers, servers, communication devices, and mainframes can be networked together and managed by a single organization. The management of these platforms often requires remote installation and configuration of software. One problem associated with the remote installation and configuration of software is assuring that only authorized code and configuration commands are installed and executed on the platforms. Failure to address this problem can result in problems ranging in seriousness from having merely incompatible or untested applications installed on the platforms to having a malicious virus introduced into the network.

After networked platforms are installed and operational, a public key for the IT management organization responsible for maintaining the platforms is stored on each platform. This permits the IT management organization to affix a digital signature to software and commands sent to each platform. A digital signature is a device by which the source and integrity of transmitted information can be verified. Before the installation of software or the execution of commands, the digital signature is verified at the platform by using the public key for the IT management organization to confirm that the software or commands came from an authorized source.

Unfortunately, in today's fast paced and heavily networked environments new platforms arriving directly from a manufacturer are constantly being connected to existing networks. These new platforms do not yet contain the public key for the IT management organization, so software and commands sent to the platform cannot yet be authenticated using public key cryptography. This is a problem when initial setup of a newly installed platform is performed remotely by an IT organization, since a few pieces of code and configuration commands must be installed on the platform to identify the responsible IT management organization by its public key for the first time. In essence, there is a window of time during which, for a newly installed platform, the standard mechanism for verifying the source and integrity of transmitted information and commands is unavailable.

For these and other reasons, there is a need for the present invention.

SUMMARY OF THE INVENTION

In one embodiment of the invention, a system includes a user platform, a communication channel, and a remote platform. The user platform authenticates information using a transformation value generated from the information. The remote platform transmits the information to the user platform via the communication channel.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram of a system for authenticating information, according to one embodiment of the invention.

FIG. **2** is a general flow diagram of a method for authenticating information, according to one embodiment of the invention.

FIG. **3** is a diagram of a representative computer, in conjunction with which embodiments of the invention may be practiced.

DETAILED DESCRIPTION OF THE INVENTION

Referring to FIG. **1**, a block diagram of one embodiment of system **100** for providing authority and integrity checks in a system lacking a public key is shown. System **100** includes remote platform **105**, user platform **110**, including transformation value generator **115**, comparison system **120**, and display system **122**. Remote platform **105** is coupled to user platform **110** by communication channel **125**. User **130** is capable of receiving input, such as credential transformation value **135**, information transformation value **140**, or credential subset transformation value **145**, from authorizing entity **150** for input into comparison system **120** of user platform **110**. Remote platform **105** is capable of receiving information **155** and credential **160**, which includes credential subset **165** from authorizing entity **150**.

Remote platform **105** is capable, in one embodiment, of staging and transmitting information **155** and credential **160** to user platform **110**. Remote platform **105** is not limited to any particular type of device and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, Such as a cell phone, or a television or radio transmitter or transceiver. Those skilled in the art will recognize that any device capable of transmitting information to user platform **110** can function as remote platform **105**.

The present invention ensures the authority and integrity of information received at user platform **110**, so it is not limited in the type of information transmitted from remote platform **105** to user platform **110**. In one embodiment of the invention, information **155** is a boot image, but those skilled in the art will recognize that the present invention is equally applicable to the transmission of information such as application software or data.

Credential **160**, in one embodiment, contains authority information, such as a digital signature or a digital signature in combination with other information, such as a digital certificate that normally accompanies transmitted information. The authority information, without a public key that designates the authorized source of the credential's digital signature installed on user platform **110**, is insufficient to check the authority of the credential. However, a credential which includes a digital signature that covers the rest of the credential can be used to check the integrity of the credential.

User platform **110** is provided for the purpose of receiving transmitted information such as information **155**, credential **160**, or information **155** and credential **160** from remote platform **105**. User platform **110** is the target device for software, commands, or data staged on remote platform **105**, and can be a computer, such as a personal computer, a server or a mainframe, or a communication device, such as a pager, a cell phone, or a television or radio receiver or transceiver. Like remote platform **105**, user platform **110** is not limited to any pailicular type of device, and those skilled in the art will recognize that any device capable of receiving information from remote platform **105** can be used in the present invention.

Communication channel **125** is provided to couple remote platform **105** to user platform **110**. Communication channel